JOURNAL OF ALGEBRA 60, 229–237 (1979)

Word Equations of Paths

MOHAN S. PUTCHA

Department of Mathematics, North Carolina State University, Raleigh, North Carolina 27650

Communicated by P. M. Cohn

Received April 12, 1976

INTRODUCTION

Let $\mathscr{D}^*$ denote the semigroup, under concatenation, of all rectifiable, piecewise continuously differentiable paths in R^n which are not constant on any subinterval and which do not form a straight line on any subinterval. Let $w_1 = w_1(x_1,..., x_t)$, $w_2 = w_2(x_1,..., x_t)$ denote two words in the letters $x_1,..., x_t$. Let $\mathscr{F} = \mathscr{F}(a_1,..., a_k)$ be a free semigroup on $a_1,..., a_k$ and suppose $u_1,..., u_t \in \mathscr{F}$ with $w_1(u_1,..., u_t) = w_2(u_1,..., u_t)$. Let $f_1,..., f_k \in \mathscr{D}^*$ and set $g_i = u_i(f_1,..., f_k) \in \mathscr{D}^*$, $i = 1,..., t$. Then clearly $w_1(g_1,..., g_t) = w_2(g_1,..., g_t)$. The main theorem of this paper is that every solution of $w_1 = w_2$ in $\mathscr{D}^*$ is obtained in this manner. In the event that $t = 2$, we are able to prove the same theorem without the assumption of differentiability.

1. PRELIMINARIES

Throughout this paper, N, Z^+, R, R^+ will denote the sets of nonnegative integers, positive integers, reals and positive reals respectively. If S is a goupoid then $S^1 = S$ if S has an identity element; $S^1 = S \cup \{1\}$ with obvious multiplication if S does not have an identity element. If Γ is a non-empty set then $\mathscr{F} = \mathscr{F}(\Gamma)$ denotes the free semigroup on Γ.

We will let $\mathscr{Y}$ denote the st of all strictly increasing continuous self-maps ϕ of $[0, 1]$ with $\phi(0) = 0$ and $\phi(1) = 1$. Let $n \in Z^+$ remain fixed throughout this paper and let $\mathscr{K}$ denote the set of all continuous functions f from $[0, 1]$ into R^n such that $f(0) = 0$ and f is not constant on any subinterval of $[0, 1]$. If $f, g \in \mathscr{K}$ then define $f \equiv g$ if $g = f \circ \phi$ for some $\phi \in \mathscr{Y}$. Then clearly $f([0, 1]) = g([0, 1])$ and $f(1) = g(1)$. It is obvious that $\equiv$ is an equivalence relation[1] on $\mathscr{K}$. Intuitively,

[1] For the purposes of this paper, several other definitions would work just as well. For instance we could impose the further constraint that ϕ be piecewise continuously differentiable.

0021-8693/79/090229-09$02.00/0

considered as function of time, we are interested in the way our path is traced but not the speed. If $f \in \mathscr{K}$, then let f^* denote the equivalence class of f and let $\mathscr{K}^* = \mathscr{K}/\equiv$. If $f, g \in \mathscr{K}$, then let $fg \in \mathscr{K}$ be defined by

$$\begin{aligned} fg(x) &= f(2x), & 0 \leqslant x \leqslant \tfrac{1}{2}, \\ &= f(1) + g(2x-1) & \tfrac{1}{2} \leqslant x \leqslant 1. \end{aligned}$$

Then $fg(1) = f(1) + g(1)$. If $f, g, f_1, g_1 \in \mathscr{K}$, $\phi_1, \phi_2 \in \mathscr{Y}$, $f_1 = f \circ \phi_1$, $g_1 = g \circ \phi_2$, then $f_1 g_1 = fg \circ \phi$ where $\phi \in \mathscr{Y}$ is given by

$$\begin{aligned} \phi(x) &= \frac{\phi_1(2x)}{2}, & 0 \leqslant x \leqslant \tfrac{1}{2}, \\ &= \frac{\phi_2(2x-1)+1}{2}, & \tfrac{1}{2} \leqslant x \leqslant 1 \end{aligned}$$

If $f, g, h \in \mathscr{K}$, then $(fg)h \circ \phi = f(gh)$ where $\phi \in \mathscr{Y}$ is given by

$$\begin{aligned} \phi(x) &= x/2, & 0 \leqslant x \leqslant \tfrac{1}{2}, \\ &= x - \tfrac{1}{4}, & \tfrac{1}{2} \leqslant x \leqslant \tfrac{3}{4}, \\ &= 2x - 1, & \tfrac{3}{4} \leqslant x \leqslant 1. \end{aligned}$$

Thus $\mathscr{K}^*$ becomes a semigroup. If $f \in \mathscr{K}$ then let $l(f)$ denote the length of f (cf. [4, p. 125]). Since f is non-constant, $l(f) > 0$. It is routine that if $f, g \in \mathscr{K}$ and $f \equiv g$, then $l(f) = l(g)$. So we let $l(f^*) = l(f)$ for $f \in \mathscr{K}$. If $f, g \in \mathscr{K}$, then it is routinely verified that $l(fg) = l(f) + l(g)$ in the extended real line.

If $0 \leqslant \alpha < \beta \leqslant 1$, $f \in \mathscr{K}$, then let $f_{[\alpha,\beta]} \in \mathscr{K}$ be defined by $f_{[\alpha,\beta]}(x) = f(\alpha + (\beta - \alpha)x) - f(\alpha)$, $x \in [0, 1]$. So $f_{[0,1]} = f$. Next let $0 \leqslant \alpha < \beta < \gamma \leqslant 1$. Then $f_{[\alpha,\gamma]} \circ \phi = f_{[\alpha,\beta]} f_{[\beta,\gamma]}$ where $\phi \in \mathscr{Y}$ is given by

$$\begin{aligned} \phi(x) &= 2\left(\frac{\beta-\alpha}{\gamma-\alpha}\right)x, & 0 \leqslant x \leqslant \tfrac{1}{2}, \\ &= \frac{(\gamma-\beta)(2x-1)+\beta-\alpha}{\gamma-\alpha}, & \tfrac{1}{2} \leqslant x \leqslant 1. \end{aligned}$$

So $f_{[\alpha,\gamma]} \equiv f_{[\alpha,\beta]} f_{[\beta,\gamma]}$. In particular $l(f_{[\alpha,\beta]}) \leqslant l(f)$ for $0 \leqslant \alpha < \beta \leqslant 1$.

LEMMA 1.1. *Let $f \in \mathscr{K}$, $0 \leqslant \alpha < \beta \leqslant 1$. Let η: $[0, 1] \to [\alpha, \beta]$ be the homeomorphism $\eta(x) = (\beta - \alpha)x + \alpha$. Then for $0 \leqslant \delta < \gamma \leqslant 1$, $g_{[\delta,\gamma]} = f_{[\eta(\delta),\eta(\gamma)]}$ where $g = f_{[\alpha,\beta]}$.*

Proof. This results from direct calculation.

COROLLARY 1.2. *Let $m \in Z^+, f_1, \ldots, f_m \in \mathscr{K}$ and set $f = f_1(f_2(\cdots(f_{m-1}f_m))\cdots)$. Then there exist $\alpha_0, \ldots, \alpha_m \in [0, 1]$ with $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_m = 1$ such that $f_{[\alpha_i, \alpha_{i+1}]} \equiv f_i$, $i = 0, \ldots, m-1$.*

Proof. We prove by induction on m. This is trivial for $m = 1$. So let $m \geqslant 2$. Let $g = f_2(\cdots(f_{m-1}f_m))\cdots)$. Then $f = f_1 g$ and therefore $f_1 = f_{[0,1/2]}$ and $g = f_{[1/2,1]}$. We are now done by Lemma 1.1 and induction.

LEMMA 1.3. *Let $f \in \mathscr{K}$, $\phi \in \mathscr{Y}$ and set $g = f \circ \phi$. Then for $0 \leqslant \alpha < \beta \leqslant 1$, $g_{[\alpha,\beta]} \equiv f_{[\phi(\alpha),\phi(\beta)]}$.*

Proof. Let $\psi \in \mathscr{Y}$ be given by

$$\psi(x) = \frac{\phi((\beta - \alpha)x + \alpha) - \phi(\alpha)}{\phi(\beta) - \phi(\alpha)}.$$

It is then easy to see that $f_{[\phi(\alpha),\phi(\beta)]} \circ \psi = g_{[\alpha,\beta]}$.

Combining Lemma 1.3 and Corollary 1.2 we obtain

COROLLARY 1.4. *Let $m \in Z^+, f, f_1, \ldots, f_m \in \mathscr{K}$ such that $f \equiv f_1 f_2 \cdots f_m$. Then there exist $\alpha_0, \ldots, \alpha_m \in [0, 1]$ with $0 = \alpha_0 < \alpha_1 < \cdots < \alpha_m = 1$ such that $f_{[\alpha_i, \alpha_{i+1}]} \equiv f_i$, $i = 0, \ldots, m-1$.*

Now let $\mathscr{M} = \{f \mid f \in \mathscr{K}, l(f) < \infty\}$. Then $\mathscr{M}$ is a subgroupoid of $\mathscr{K}$. If $f \in \mathscr{M}$ and $\alpha, \beta \in [0, 1]$, $\alpha < \beta$, then $f_{[\alpha,\beta]} \in \mathscr{M}$. If $f, g \in \mathscr{M}$, then $l(fg) = l(f) + l(g) > l(f)$. In $\mathscr{M}^1$, set $l(1) = 0$. Also for $\alpha \in [0, 1]$, $f \in \mathscr{M}$, define $f_{[\alpha,\alpha]} = 1$. $\mathscr{M}^* = \mathscr{M}/\equiv$ is a subsemigroup of $\mathscr{K}^*$.

DEFINITION. Let $f, g \in \mathscr{M}$. Then

(1) $f \mid_i g$ (f is an initial segment of g) if $g \equiv f g_1$ for some $g_1 \in \mathscr{M}^1$. Then we also define $f^* \mid_i g^*$.

(2) $f \mid_f g$ (f is a final segment of g) if $g \equiv g_1 f$ for some $g_1 \in \mathscr{M}^1$. Then we also define $f^* \mid_f g^*$.

Let $f \in \mathscr{M}$, α, α_1, β, $\beta_1 \in \mathscr{F}^1$ such that $0 \leqslant \alpha \leqslant \alpha_1 < \beta_1 \leqslant \beta \leqslant 1$. Then $f_{[\alpha,\beta]} \equiv f_{[\alpha,\alpha_1]} f_{[\alpha_1,\beta_1]} f_{[\beta_1,\beta]}$. So $l(f_{[\alpha_1,\beta_1]}) \leqslant l(f_{[\alpha,\beta]})$. Also $l(f_{[\alpha_1,\beta_1]}) = l(f_{[\alpha,\beta]})$ if and only if $\alpha = \alpha_1$ and $\beta = \beta_1$. Let $f_1, f_2, g_1, g_2 \in \mathscr{M}$ such that $f_1 f_2 \equiv g_1 g_2$. Assume $l(f_1) \leqslant l(f_2)$. Let $f = f_1 f_2$. By Corollary 1.4, there exist $\alpha, \beta \in (0, 1]$ such that $f_1 \equiv f_{[0,\alpha]}$ and $g_1 \equiv f_{[0,\beta]}$. Since $l(f_1) \leqslant l(g_1)$ we obtain from the above that $\alpha \leqslant \beta$ and $f_1 \mid_i g_1$. Also $l(f_1) = l(g_1)$ implies $\alpha = \beta$ and hence $f_1 \equiv g_1$. In particular $f_1 g_2 \equiv g_1 g_2$ implies $f_1 \equiv g_1$. The above arguments along with their duals imply the following analogue of Levi's lemma for free semigroups.

Lemma 1.5. *$\mathscr{M}^*$ is a cancellative semigroup. Let $f_1, f_2, g_1, g_2 \in \mathscr{M}$ such that $f_1 f_2 \equiv g_1 g_2$ Then exactly one of the following occurs.*

(1) $l(f_1) < l(g_1)$, $l(g_2) < l(f_2)$, $f_1 |_i\, g_1$ *and* $g_2 |_f\, f_2$.

(2) $l(g_1) < l(f_1)$, $l(f_2) < l(g_2)$, $g_1 |_i\, f_1$ *and* $f_2 |_f\, g_2$.

(3) $f_1 \equiv g_1$ *and* $f_2 \equiv g_2$.

Definition. $f \in \mathscr{M}$ (and also f^*) is a line if $f = \nu\phi$ for some $\phi \in \mathscr{Y}$, $\nu \in R^n$ with $\nu \neq 0$.

If $f, g \in \mathscr{M}$, $g |_i f$ and if f is a line, then so are g and fg. Let $\nu \in R^n$, $\nu \neq 0$, ϕ: $[0, 1] \to R$ strictly increasing such that $\phi(0) = 0$. Then $\nu\phi = \phi(1)\,\nu\phi_1$ where $\phi_1 = \phi/\phi(1) \in \mathscr{Y}$. So $\nu\phi$ is a line.

Lemma 1.6. *Let $f \in \mathscr{M}$ such that for any $\alpha \in (0, 1)$ and any $M \in Z^+$, there exist $m \in Z^+$, $\beta \in [\alpha, 1]$, $g \in \mathscr{M}$ such that $m \geqslant M$ and $g^m \equiv f_{[0,\beta]}$. Then f is a line.*

Proof. Let $L = \{tf(1) \mid 0 \leqslant t \leqslant 1\}$. We will first show that $f([0, 1]) \subseteq L$. Let $x \in (0, 1)$. Choose $\epsilon > 0$. There exists $\alpha \in (0, 1)$ such that for all $y \in [0, \alpha]$, $|f(y)| < \epsilon$. Choose $M \in Z^+$ such that $l(f)/M < l(f_{[0,\alpha]})$. There exists $\xi \in (x, 1)$ such that for all $y \in [\xi, 1]$, $|f(y) - f(1)| < \epsilon$. There exist $m \in Z^+$, $\beta \in [\xi, 1]$, $g \in \mathscr{M}$ such that $m \geqslant M$ and $g^m \equiv f_{[0,\beta]}$. So $g \equiv f_{[0,\delta]}$ for some $\delta \in (0, 1]$. Then

$$l(f([0,\delta])) = l(g)\, \frac{l(f_{[0,\beta]})}{m} \leqslant \frac{l(f)}{m} < l(f_{[0,\alpha]}).$$

So $\delta < \alpha$. In particular, for all $z \in [0, 1]$, $|g(z)| < \epsilon$. By Lemma 1.1 and Corollary 1.4, there exist $\gamma_0, \gamma_1, ..., \gamma_m \in [0, \beta]$ such that $0 = \gamma_0 < \gamma_1 < \cdots < \gamma_m = \beta$ and $f_{[\gamma_i, \gamma_{i+1}]} \equiv g$, $i = 0, ..., m-1$. It follows that $f(\gamma_i) = i/m\, f(\beta)$, $i = 0, ..., m-1$. Now $x \in [\gamma_j, \gamma_{j+1}]$ for some j. Then $f(x) - f(\gamma_j) = g(z)$ for some $z \in [0, 1]$. In particular $|f(x) - f(\gamma_j)| < \epsilon$. Since $\beta \geqslant \xi$, $|f(\beta) - f(1)| < \epsilon$. So $|f(\gamma_j) - j/m\, f(1)| = j/m\, |f(\beta) - f(1)| < \epsilon$. Thus $|f(x) - j/m\, f(1)| < 2\epsilon$, $j/m\, f(1) \in L$. Since ϵ is arbitrary and L is closed, $f(x) \in L$. Thus $f([0, 1]) \subseteq L$. So there exists ϕ: $[0, 1] \to [0, 1]$ with $\phi(0) = 0$, $\phi(1) = 1$ such that $f = f(1)\phi$. Since f is not constant, $f(1) \neq 0$. Then since f is continuous, so is ϕ. We show that ϕ is increasing. Let $x, y \in (0, 1)$, $x < y$ and let $\epsilon > 0$. There exists $\alpha \in (0, 1)$ such that $|f(z)| < \epsilon$ for all $z \in [0, \alpha]$. Choose $M \in Z^+$ such that $l(f)/M < l(f_{[0,\alpha]})$ There exist $\beta \in [y, 1]$, $g \in \mathscr{M}$, $m \in Z^+$ such that $m \geqslant M$ and $g^m \equiv f_{[0,\beta]}$. As before, we see that $|g(z)| < \epsilon$ for all $z \in [0, 1]$. Also as before there exist γ_0, $\gamma_1, ..., \gamma_m \in [0, \beta]$ such that $0 = \gamma_0 < \gamma_1 < \cdots < \gamma_m = \beta$ and $f_{[\gamma_i, \gamma_{i+1}]} \equiv g$, $f(\gamma_i) = i/m\, f(\beta)$, $i = 0, ..., m-1$. Now $x \in [\gamma_j, \gamma_{j+1}]$, $y \in [\gamma_k, \gamma_{k+1}]$ for some j, k. Since $x < y$, we get $j \leqslant k$. Also as before $|f(x) - f(\gamma_j)| < \epsilon$ and $|f(y) - f(\gamma_k)| < \epsilon$. Hence $|\phi(x) - (j/m)\,\phi(\beta)| < \epsilon/|f(1)|$ and $|\phi(y) - (k/m)\,\phi(\beta)| < \epsilon/|f(1)|$. Since $j \leqslant k$, $\phi(\beta) \geqslant 0$, we get $\phi(x) - \phi(y) < 2\epsilon/|f(1)|$. Since ϵ is arbitrary, $\phi(x) \leqslant \phi(y)$. Thus ϕ is increasing. Since f is non-constant on any subinterval of $[0, 1]$, ϕ is strictly increasing. Thus f is a line.

Following the terminology of free semigroups, call $f \in \mathscr{M}$ *primitive* if $f \not\equiv g^m$ for any $g \in \mathscr{M}$, $m \in Z^+$, $m \geqslant 2$. We obtain by Lemma 1.6,

COROLLARY 1.7. *Let $f \in \mathscr{M}$. Then either $f \equiv g^m$ for some primitive $g \in \mathscr{M}$, $m \in Z^+$, or else f is a line.*

LEMMA 1.8. *Let f, $g \in \mathscr{M}$ such that $fg \equiv gf$. Then either exist $h \in \mathscr{M}$, i, $j \in Z^+$ such that $f \equiv h^i$, $g \equiv h^j$, or else fg is a line.*

Proof. Let $C = \{(f, g) | f, g \in \mathscr{M}, fg \equiv gf, f, g$ are not $\equiv$ powers of a common element in $\mathscr{M}\}$. Let $(f, g) \in C$. Then $f \not\equiv g$ and by symmetry we may assume $l(f) < l(g)$. So $f \,|_i\, g$ and since g is not $\equiv$ a power of f there exist $i \in Z^+$, $g_1 \in \mathscr{M}$ such that $g \equiv f^i g_1$ and $f \nmid_i g_1$. Then $(f, g_1) \in C$. So $l(g_1) < l(f)$. Thus $f \equiv g_1 f_1$ for some $f_1 \in \mathscr{M}$. So $(f_1, g_1) \in C$. Also $fg \equiv f_1^{i+1} g_1^{i+2}$. Repeating this process for (f_1, g_1) and continuing, we see that there exists a sequence of elements $\{(f_k, g_k)\}$ in C, sequences of positive integers $\{\alpha_k\}$, $\{\beta_k\}$ such that $\alpha_k \to \infty$, $\beta_k \to \infty$ and for each k, $fg \equiv f_k^{\alpha_k} g_k^{\beta_k} \equiv g_k^{\beta_k} f_k^{\alpha_k}$. So without loss of generality (and going to a subsequence if necessary) we can assume that $l(f_k^{\alpha_k}) \geqslant l(g_k^{\beta_k})$ for all k. Since $l(f) < l(g)$ we obtain $l(f_k^{\alpha_k}) > l(f)$ for all k. We will now show that f satisfies the hypothesis of Lemma 1.6. So let $\mu \in (0, 1)$, $M \in Z^+$. Let $\epsilon = \min\{l(f)/(M+1), l(f_{[\mu,1]})\}$. Then $\epsilon > 0$. There exists α_k such that $l(f_k) \leqslant l(f)/\alpha_k < \epsilon$. Now $f \,|_i\, f_k^{\alpha_k}$. So there exist $m \in N$, h_1, $h_2 \in \mathscr{M}^1$ such that $m \leqslant \alpha_k$, $f \equiv f_k{}^m h_1$ and $h_1 h_2 \equiv f_k$. So $l(f)/(m+1) \leqslant l(f_k) \leqslant l(f)/(M+1)$. So $M \leqslant m$. Also $l(h_1) \leqslant l(f_k) \leqslant l(f_{[\mu,1]})$. Now $h_1 \equiv f_{[\nu,1]}$ for some $\nu \in [0, 1]$. Since $l(f_{[\nu,1]}) \leqslant l(f_{[\mu,1]})$, we get that $\nu \geqslant \mu$. Also $f_k^m \equiv f_{[0,\nu]}$. Thus the hypothesis of Lemma 1.6 is satisfied and f is a line. But $g \equiv f^i g_1$ and $g_1 \,|_i\, f$. So $fg \equiv f^{i+1} g_1$ is also a line.

COROLLARY 1.9. *Let u, $v \in \mathscr{M}^*$, i, $j \in Z^+$ such that $u^i = v^j$. Then there exist $w \in \mathscr{M}^*$, k, $m \in Z^+$ such that $w^k = u$ and $w^m = v$.*

Proof. If u is a line then so is v and in the same direction. But the subsemigroup of lines in a particular direction is easily seen to be isomorphic to the positive reals under addition. So in that case the result holds trivially. So assume u, v are not lines. If $l(u) = l(v)$ then $u = v$. So by symmetry let $l(u) < l(v)$. Then $v = uv_1$ for some $v_1 \in \mathscr{M}^*$. So $i > 1$ and $u^{i-1} = v_1(uv_1)^{j-1}$. So $u^i = u^{i-1}u = (v_1 u)^j$. But also $u^i = v^j = (uv_1)^j$. Thus $uv_1 = v_1 u$. Since u is not a line, u and v_1 are powers of a common $w \in \mathscr{M}^*$. Hence so are u and v.

THEOREM 1.10. *Let $w_1 = w_1(A, B)$, $w_2 = w_2(A, B) \in \mathscr{F}(A, B)$ such that w_1 starts with A and w_2 starts with B. Suppose u, $v \in \mathscr{M}^*$ and $w_1(u, v) = w_2(u, v)$.*

Then either there exist $a \in \mathcal{M}^*$, $i, j \in Z^+$ such that $u = a^i$ and $v = a^j$ or else uv is a line.

Proof. First assume that B occurs in w_1 and A occurs in w_2. There exist $\alpha, \beta \in Z^+$ such that $w_1 = A^\alpha B...$ and $w_2 = B^\beta A....$ Then $u^\alpha v... = v^\beta u....$ By symmetry let $l(u) \leqslant l(v)$. So there exist $\gamma \in Z^+$, $v_1 \in (\mathcal{M}^*)^1$ such that $v = u^\gamma v_1$, $u \nmid_i v_1$. Then $u^\alpha v_1... = v_1 u....$ Since $u \nmid_i v_1$, there exists $u_1 \in \mathcal{M}^*$ such that $u = v_1 u_1$. Then we obtain $u_1 v_1 = v_1 u_1$. So either $v_1 = 1$ or else Lemma 1.8 applies. In either case we are done. Next assume $w_1 = A^\alpha B...$, $w_2 = B^\beta$, $\alpha, \beta \in Z^+$. Then $u^\alpha v... = v^\beta$ and $\beta \geqslant 2$. If $l(u) \leqslant l(v)$, then the above argument works again. So let $l(v) < l(u)$. If u is a power of v, we are done. So let $u = v^\gamma u_1$, $v \nmid_i u_1$, for some $\gamma \in Z^+$, $u_1 \in \mathcal{M}^*$. Then $\gamma < \beta$ and $u_1 v... = v^{\beta-\gamma}$. Then $\beta - \gamma \geqslant 2$ and $v = u_1 v_1$ for some $v_1 \in \mathcal{M}^*$. Hence $u_1 v_1 = v_1 u_1$ and we are done by Lemma 1.8. The final possibility is that $w_1 = A^\alpha$ and $w_2 = B^\beta$ for some $\alpha, \beta \in Z^+$. Then $u^\alpha = v^\beta$ and we are done by Corollary 1.9.

2. The Main Theorem

Let $\mathcal{D}$ denote the subgroupoid of $\mathcal{M}$ consisting of all $f \in \mathcal{M}$ such that f is piecewise continuously differentiable (in the sense of [5, p. 127]) and $f_{[\alpha,\beta]}$ is not a line for any $\alpha, \beta \in [0, 1]$ with $\alpha < \beta$. If $\alpha, \beta \in [0, 1]$, $\alpha < \beta$ and if $f \in \mathcal{D}$ then so does $f_{[\alpha,\beta]}$. In particular if $f, g \in \mathcal{D}$ and if $f \mid_i g$ in $\mathcal{M}$, then by Corollary 1.4, $g \equiv fg_1$ for some $g_1 \in \mathcal{D}^1$. A similar statement holds with respect to $\mid_f$. Of course it can happen that $f \in \mathcal{D}$, $g \in \mathcal{M}$, $f \equiv g$, but $g \notin \mathcal{D}$. Let $\mathcal{D}^* = \{f^* \mid f \in \mathcal{D}\} \simeq \mathcal{D}/\equiv$. Then $\mathcal{D}^*$ is a subsemigroup of $\mathcal{M}^*$. There exist two books [1, 2] on equations in free semigroups. We use ideas from these freely. If $A \in R^n$, then let $RA = \{xA \mid x \in R\}$.

Theorem 2.1. *Let $w_1 = w_1(X_1, ..., X_t)$, $w_2 = w_2(X_1, ..., X_t) \in \mathcal{F}(X_1, ..., X_t)$. Let $F_1, ..., F_t \in \mathcal{D}$ such that $w_1(F_1, ..., F_t) \equiv w_2(F_1, ..., F_t)$. Then there exists a free semigroup $\mathcal{F}(Y_1, ..., Y_s)$, $s \leqslant t$, $u_1, ..., u_t \in \mathcal{F}(Y_1, ..., Y_s)$, $T_1, ..., T_s \in \mathcal{D}$ such that $w_1(u_1, ..., u_t) = w_2(u_1, ..., u_t)$ and $F_i \equiv u_i(T_1, ..., T_s)$, $i = 1, ..., t$.*

Proof. We prove by induction on t. The theorem is trivial for $t = 1$. So let $t > 1$. We can assume without loss of generality that w_1, w_2 start with different letters and that $w_1 w_2$ involves each X_i at least once. Let X_i appear $m_i^{(0)}$ times in $w_1 w_2$, $i = 1, ..., t$. So $m_i^{(0)} \in Z^+$, $i = 1, ..., t$. Set $F_i^{(0)} = F_i$ for $i = 1, ..., t$. We assume that the conclusion of the theorem is false and obtain a contradiction. Let $H = w_1 w_2(F_1^{(0)}, ..., F_t^{(0)}) \in \mathcal{D}$ with the product being taken in some association. Let $w_1 = X_i ...$, $w_2 = X_j ...$, $i \neq j$. So

$$F_i^{(0)} \cdots \equiv F_j^{(0)} \cdots . \tag{1}$$

If $F_i^{(0)} \equiv F_j^{(0)}$, we see by our induction hypothesis that the conclusion of the theorem holds, a contradiction. So by symmetry let $l(F_i^{(0)}) < l(F_j^{(0)})$. Then the left hand side of (1) consists of more than just $F_i^{(0)}$ (say it looks like $F_i^{(0)}F_k^{(0)}...$) and $F_j^{(0)} \equiv F_i^{(0)}F_j^{(1)}$ for some $F_j^{(1)} \in \mathscr{D}$. Set $F_r^{(1)} = F_r^{(0)}$ for $r \neq j$. Retracing, we see that $H \equiv$ a word in $F_1^{(1)},..., F_t^{(1)}$. If $F_r^{(1)}$ appears $m_r^{(1)}$ times in this word, then $m_r^{(1)} = m_r^{(0)}$ for $r \neq i$ and $m_i^{(1)} = m_i^{(0)} + m_j^{(0)}$. So $\sum_{r=1}^t m_r^{(0)} < \sum_{r=1}^t m_r^{(1)}$. Also $F_r^{(1)} |_f F_r^{(0)}$, $m_r^{(1)} \geqslant m_r^{(0)}$, $r = 1,..., t$. If $k \neq j$, then (1) becomes

$$F_k^{(1)} \cdots \equiv F_j^{(1)} \cdots . \tag{2}$$

If $k = j$, then (1) becomes

$$F_i^{(1)}F_j^{(1)} \cdots \equiv F_j^{(1)} \cdots . \tag{3}$$

We can repeat this process for (2) and (3). Since we are assuming that the conclusion of the theorem is false we can (because of the induction hypothesis) continue this process indefinitely so as to obtain sequences $\{F_r^{(\alpha)}\}$[2]) in $\mathscr{D}$ and $\{m_r^{(\alpha)}\}$ in Z^+, $r = 1,..., t$ such that $F_r^{(\alpha+1)} |_f F_r^{(\alpha)}$, $m_r^{(\alpha+1)} \geqslant m_r^{(\alpha)}$, $r = 1,..., t$, $\sum_{r=1}^t m_r^{(\alpha)} < \sum_{r=1}^t m_r^{(\alpha+1)}$ and $H \equiv$ a word in $F_1^{(\alpha)},..., F_t^{(\alpha)}$ with each $F_r^{(\alpha)}$ appearing $m_r^{(\alpha)}$ times, $\alpha \in N$. Also for $\alpha, \beta \in N$, $\alpha < \beta$, $F_r^{(\alpha)}$ is a word in some of $F_1^{(\beta)},..., F_t^{(\beta)}$, $r = 1,..., t$. Since $\sum_{r=1}^t m_r^{(\alpha)} \to \infty$, at least one $m_\nu^{(\alpha)} \to \infty$. So $l(F_\nu^{(\alpha)}) \to 0$. Let $\Omega = \{\mu \mid \mu \in \{1,..., t\}, l(F_\mu^{(\alpha)}) \to 0\}$. There exists $\lambda \in R^+$ such that $l(F_\mu^{(\alpha)}) > \lambda$ for all $\mu \in \{1,..., t\} \backslash \Omega$, $\alpha \in N$. There exists $\beta \in N$ such that $l(F_\nu^{(\beta)}) < \lambda$. So for $\alpha > \beta$, $F_\nu^{(\beta)}$ is $\equiv$ a word in $F_\mu^{(\alpha)}$'s, $\mu \in \Omega$. Let $F = F_\nu^{(\beta)}$. So by Corollary 1.4, for each $x \in [0, 1]$ and $\alpha \in N$, $\alpha > \beta$, there exist $c_1, c_2 \in [0, 1]$, $c_1 < c_2$ such that $x \in [c_1, c_2]$ and $F_{[c_1, c_2]} \equiv F_\mu^{(\alpha)}$ for some $\mu \in \Omega$. Soince Ω is finite, for any given $x \in [0, 1]$ there exist $\eta(x) \in \Omega$ and a sequence of integers, $\beta < \alpha_1 < \alpha_2 < \cdots$ such that for each $r \in Z^+$, there exist $c_1, c_2 \in [0, 1]$ such that $c_1 < c_2$, $x \in [c_1, c_2]$ and $F_{[c_1, c_2]} \equiv F_{\eta(x)}^{(\alpha_r)}$ So η: $[0, 1] \to \Omega$.

There exist $c, d \in [0, 1]$, $c < d$ such that the derivative F' exists, is $\neq 0$, and is continuous on $[c, d]$. Let $x, y \in (c, d)$ such that $\eta(x) = \eta(y)$. Let $G = F_{\eta(x)}$ and let $A = F'(x)$, $B = F'(y)$. So $A \neq 0$, $B \neq 0$, $A, B \in R^n$. We claim that $B \in RA$. Let $K = \max_{y \in [c,d]} |F'(y)|$. Then $K > 0$. Let $\epsilon > 0$. There exists $\delta > 0$ such that $\delta < \epsilon$, $\delta < |A|/2$, $\delta < |A| \epsilon/2K$. Let $F = (f_1,..., f_n)$, $A = (A_1,..., A_n)$, $B = (B_1,..., B_n)$. Then $F' = (f'_1,..., f'_n)$ and each f'_p is continuous and real valued on $[c, d]$. So there exist $c_1, c_2, d_1, d_2 \in (c, d)$, $c_1 < c_2$, $d_1 < d_2$ with $x \in (c_1, c_2)$, $y \in (d_1, d_2)$ such that for any $z_1 \in [c_1, c_2]$, $z_2 \in [d_1, d_2]$, $|f'_p(z_1) - A_p| < \delta/(n)^{1/2}$ and $|f'_p(z_2) - B_p| < \delta/(n)^{1/2}$, $p = 1,..., n$. Now let a_1, $a_2 \in [c_1, c_2]$, $a_1 < a_2$. By the mean value theorem there exist $z_1,..., z_n \in (a_1, a_2)$ such that

$$f_p(z'_p) = \frac{f_p(a_2) - f_p(a_1)}{a_2 - a_1}, \qquad p = 1,..., n.$$

[2] This notation has nothing to do with higher order derivatives.

It follows from the above that

$$\left| \frac{F(a_2) - F(a_1)}{a_2 - a_1} - A \right| < \delta \qquad \text{for any} \quad a_1, a_2 \in [c_1, c_2], a_1 < a_2. \tag{4}$$

Similarly we have

$$\left| \frac{F(b_2) - F(b_1)}{b_2 - b_1} - B \right| < \delta \qquad \text{for any} \quad b_1, b_2 \in [d_1, d_2], b_1 < b_2. \tag{5}$$

Now let $\xi = \min\{l(F_{[c_1,x]}), l(F_{[x,c_2]}), l(F_{[d_1,y]}), l(F_{[y,d_2]})\}$. Then $\xi > 0$ and there exist $c_3, c_4 \in [0, 1]$, $\alpha \in Z^+$ such that $c_3 < c_4$, $x \in [c_3, c_4]$, $F_{[c_3,c_4]} = G^{(\alpha)}$ and $l(G^{(\alpha)}) < \xi$. So $l(F_{[c_3,x]}) < l(F_{[c_1,x]})$ and $l(F_{[x,c_4]}) < l(F_{[x,c_2]})$. It follows that $[c_3, c_4] \subsetneq [c_1, c_2]$. There exist $\gamma \in Z^+$, $\gamma > \alpha$, $d_3, d_4 \in [0, 1]$ such that $d_3 < d_4$, $y \in [d_3, d_4]$, $F_{[d_3,d_4]} = G^{(\gamma)}$, and $l(G^{(\gamma)}) < \xi$. So as above, $[d_3, d_4] \subsetneq [d_1, d_2]$. Since $\alpha < \gamma$, $G^{(\gamma)} |_f G^{(\alpha)} = F_{[c_3,c_4]}$. So there exists $a \in [c_3, c_4)$ such that $F_{[a,c_4]} = G^{(\gamma)}$. So $F_{[a,c_4]} = F_{[d_3,d_4]}$. Hence

$$F(c_4) - F(a) = F_{[a,c_4]}(1) = F_{[d_3,d_4]}(1) = F(d_4) - F(d_3). \tag{6}$$

Let $M = (d_4 - d_3)/(c_4 - a)$. Then by (4) and (6) we get

$$\left| M \frac{F(d_4) - F(d_3)}{d_4 - d_3} - A \right| < \delta < \frac{|A|}{2}. \tag{7}$$

By [4, Theorem 5.20],

$$\left| \frac{F(d_4) - F(d_3)}{d_4 - d_3} \right| \leqslant K.$$

So

$$\begin{aligned} |A| - K|M| &\leqslant |A| - \left| \frac{F(d_4) - F(d_3)}{d_4 - d_3} \right| |M| \\ &\leqslant \left| \frac{F(d_4) - F(d_3)}{d_4 - d_3} M - A \right| < \frac{|A|}{2}. \end{aligned}$$

Hence $1/|M| < 2K/|A|$. Thus multiplying (7) by $1/|M|$ we get

$$\left| \frac{F(d_4) - F(d_3)}{d_4 - d_3} - \frac{1}{M} A \right| < \frac{2K\delta}{|A|} < \epsilon.$$

Also, by (5),

$$\left| \frac{F(d_4) - F(d_3)}{d_4 - d_3} - B \right| < \delta < \epsilon.$$

So $| B - (1/M)A | < 2\epsilon$. Since ϵ is arbitrary and RA is closed, $B \in RA$. Thus our claim is established. Since Ω is finite, there exist non-zero $A_1, ..., A_\theta \in R^n$ such that $A_p \notin RA_q$ for $p \neq q$ and so that for any $x \in (c, d)$, $F'(x) \in RA_p$ for some p. Now fix $x \in (c, d)$ and let $F'(x) = \delta A_p$, $\delta \in R$, $\delta \neq 0$. There exists $\epsilon \in R^+$ such that for all $\xi \in R$, $| F'(x) - \xi A_q | \geqslant \epsilon$ for $q \in \{1, ..., \theta\}$, $q \neq p$. There exist $c', d' \in (c, d)$, $c' < d'$, such that $x \in (c', d')$ and for all $y \in [c', d']$, $| F'(y) - F'(x)| < \epsilon$. It follows that for all $y \in [c', d']$, $F'(y) \in RA_p$. So there exists a function ϕ: $[c', d'] \to R$ such that $F' = A_p \phi$ on $[c', d']$. Since $A_p \neq 0$ and F' is continuous we see that ϕ is continuous. Since $F' \neq 0$, $\phi \neq 0$. So there exist $c'', d'' \in [c', d']$, $c'' < d''$, such that $\phi > 0$ on all of $[c'', d'']$ or $\phi < 0$ on all of $[c'', d'']$. We might as well assume the former case—since otherwise, we can replace ϕ by $-\phi$ and A_p by $-A_p$ in the following. Let ψ: $[c'', d''] \to R$ be given by $\psi(z) = \int_{c''}^{z} \phi$. Then ψ is strictly increasing on $[c'', d'']$, $\psi(c'') = 0$. Also, for $z \in [c'', d'']$, $F(z) - F(c'') = \int_{c''}^{z} F' = A_p \psi(z)$. It follows that $F_{[c'', d'']} = A_p \psi_1$ where $\psi_1 : [0, 1] \to R$ is given by $\psi_1(y) = \psi(c'' + (d'' - c'')y)$. Then $\psi_1(0) = 0$ and ψ_1 is strictly increasing. Hence $F_{[c'', d'']}$ is a line, a contradiction. This proves the theorem.

Remark. Let $\mathscr{A}$ be the subgroupoid of $\mathscr{M}$ consisting of all $f \in \mathscr{M}$ such that for all $\alpha, \beta \in [0, 1]$, $\alpha < \beta$, $f_{[\alpha, \beta]}$ is not a line and there exist $\alpha', \beta' \in [\alpha, \beta]$, $\alpha' < \beta'$ such that f is continuously differentiable on $[\alpha', \beta']$. Then our proof shows that Theorem 2.1 remains valid for $\mathscr{A}$. Let $\mathscr{B}$ be a subset of $\mathscr{A}$ such that for all $f \in \mathscr{B}$, $\alpha \in [0, 1)$, $f_{[\alpha, 1]} \in \mathscr{B}$. Then using results of [2] it can be shown that Theorem 2.1 holds for $\mathscr{B}$. The same is true if instead $f_{[0, \beta]} \in \mathscr{B}$ whenever $\beta \in (0, 1]$ and $f \in \mathscr{B}$.

If Γ is a non-empty set, then let $\mathscr{F}_R(\Gamma)$ denote the free product of $| \Gamma |$ copies of R^+ under addition (cf. [3, p. 411]).

Problem. Theorem 2.1 tells us that all the solutions of a t-variable word equation in $\mathscr{D}$ can be derived from the solutions of the same equation in the free semigroup on t letters. Let $\mathscr{D}_1$ be the subgroupoid of $\mathscr{M}$ consisting of all piecewise continuously differentiable paths in $\mathscr{M}$. Can all the solutions of a t-variable word equation in $\mathscr{D}_1$ be derived from the solutions of the same equation in $\mathscr{F}_R(Y_1, ..., Y_t)$? How about $\mathscr{M}$?

References

1. Ju. I. Hmelevskii, "Equations in the Free Semigroup," Trudy Mat. Inst. Steklova, No. 107 (1971) [in Russian].
2. A. Lentin, "Équations dans les monoïdes libres," Gauthier–Villars, Mouton, 1972.
3. E. S. Ljapin, "Semigroups," Amer. Math. Soc. Translations, Amer. Math. Soc., Providence, R. I., 1963; translation of "Polugruppy," 1960.
4. W. Rudin, "Principles of Mathematical Analysis," 2nd ed., McGraw–Hill, New York, 1964.
5. W. Rudin, "Real and Complex Analysis," 2nd ed., McGraw–Hill, New York, 1974.